圣博润
SBR-info

LanSecS®

日志审计系统

产品概述

LanSecS® 日志审计系统（简称LAS）通过收集并分析主机、安全设备、网络设备、数据库等运行过程中产生的日志，发现网络中的违规行为和安全问题，完整还原并呈现安全事件。补充提供日志的收集汇总、集中存储、智能分析、告警报表等功能，可满足安全合规性审计需求和安全分析需求。

产品功能

- **日志采集**

  采用分布式消息引擎对网络设备、安全设备、主机操作系统、数据库、中间件和应用系统等产生的日志进行收集与标准化解析。

- **日志存储**

  内置分布式非关系型数据库，可将海量日志集中存储，存储时间满足网络安全法要求。

- **日志范式化**

  内置主流厂商设备的范式化策略，非主流厂商设备日志范式化可在界面自定义，系统支持通过策略包导入的方式扩展范式化策略。

- **日志分析**

  通过对海量日志的去重、过滤、关联等分析，提供可视化的分析结果及时展现。

- **告警管理**

  通过告警管理可对安全事件分级并以邮件、短信、微信等方式提供告警。

- **资产管理**

  可对资产进行分组、分域管理，能够从资产维度查询事件信息、关联告警信息、关联事件等。

- **报表管理**

  内置多种合规性报表，可按照天、月度、季度、年度等时间周期生成报表，还可以按照应用场景，以目录树的方式汇总成综合性报告。

产品特点

- **海量、异构日志快速处理**

  采用业界最新的大数据技术和独有的基于机器学习的范式化技术，可快速从各类异构资产日志、事件中抽取关键性信息完成快速准确的标准化解析与映射。处理过程中可定义统一的安全策略，按照不同维度和事件级别等条件组合进行日志格式重定义。

提供灵活可扩展的日志范式化策略

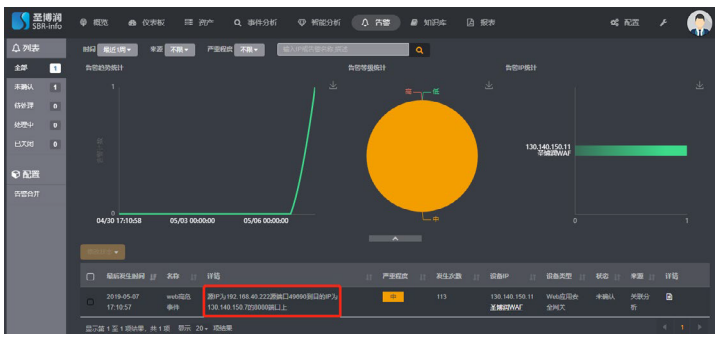
支持可视化的日志范式化策略编辑，可自定义扩展范式化字段、映射表等，自定义字段也可被安全分析规则引用。系统还支持二级范式化，可对已范式化的内容进行详细范式化。

提供多种分析方法及分析模型

内置多种关联分析、审计分析规则与模型，通过简单引用和配置便可真实还原网络中的安全事件。

提供安全事件的快速溯源

支持从告警到安全事件的快速追踪，以便及时详细了解安全事件前因后果。通过对事件的追踪可快速溯源，准确定位到原始日志。



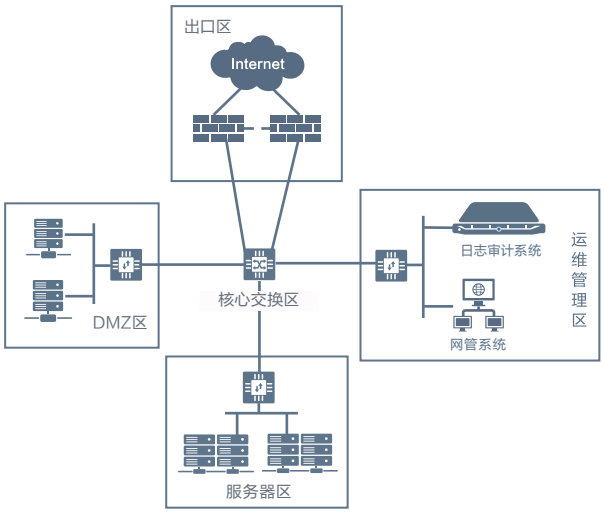
灵活易建的大屏展示

仪表板支持自定义，组件可任意摆放、调整大小，可灵活快速的构建所需的大屏展示效果。

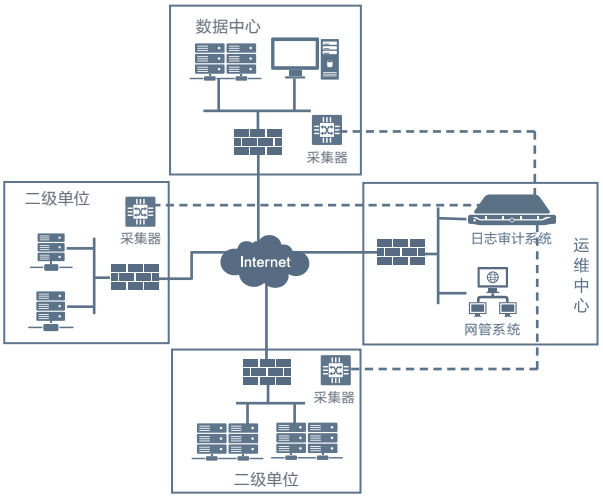
产品部署

LanSecS®日志审计系统采用旁路的方式接入用户网络，支持单级部署、多级部署、集群部署等多种部署方式，用户可根据自身实际需求来选择合适的部署方式。

典型部署方式：单级部署、多级部署



单级部署



多级部署

产品规格

产品型号	产品规格
LAS-SV50	软件版，系统自带 50 个 License 授权，License 授权可扩充。
LAS-P500	1U 标准机架式设备，单电源，License 授权数量不限制，每秒 500 条日志入库条件下日志可保存 6 个月以上。
LAS-P1000	1U 标准机架式设备，单电源，License 授权数量不限制，每秒 1000 条日志入库条件下日志可保存 6 个月以上。
LAS-P2000	2U 标准机架式设备，冗余电源，License 授权数量不限制，每秒 2000 条日志入库条件下日志可保存 6 个月以上。
LAS-P4000	2U 标准机架式设备，冗余电源，License 授权数量不限制，每秒 4000 条日志入库条件下日志可保存 6 个月以上。

★ 产品规格可能会随市场需求调整，请及时联系以获取最新规格参数。

地址：北京市海淀区高梁桥斜街 59 号院 2 号楼 3 层 / 邮编：100044 / 技术支持热线：800-810-2332 / 400-966-2332

电话：010-82138088 / 技术支持邮箱：support@sbr-info.com / 网址：www.sbr-info.com

201907